UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/930,029 | 08/14/2001 | William B. Sweet | 00131-000100000 | 3170 |

31064 7590 06/22/2009

WIESNER & ASSOCIATES
366 CAMBRIDGE AVENUE
PALO ALTO, CA 94306

| EXAMINER | |
|---|---|
| POPHAM, JEFFREY D | |
| ART UNIT | PAPER NUMBER |
| 2437 | |
| MAIL DATE | DELIVERY MODE |
| 06/22/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/930,029 | SWEET ET AL. | |
| | Examiner | Art Unit | |
| | JEFFREY D. POPHAM | 2437 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *10 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-22 and 52-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 52-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

***Remarks***

Claims 1-22 and 52-66 are pending.

***Response to Amendment***

1. The amended claims include various issues with claim markings. For example, claims 64-66 are stated as being "original", however, such claims were newly added in the response dated 4/16/2008. Claims 60-62 state that they are "new", but were previously presented. Claim 52 is referred to as previously presented, but includes amendments that are not even highlighted (e.g. underlining for added amendments and striking through for removed portions, claim 52 including both removed and added portions, yet not containing either underling or strike-through for any of them).

The Examiner will not review every claim for amendments such as those that are not highlighted in claim 52, but rather will take previously presented and original to mean just that, with the exception of claim 52, which will be rejected in its amended form (even though the amendment was not underlined or even noted in the claim designation, claim 52 has been reviewed for 101 issues, as Applicant stated that the claim was amended in the remarks). Proper claim designations are required, as well as properly underlining added limitations and striking through removed limitations. If any amendments were made to other claims not referred to as “currently amended”, such amendments will not be included in the rejections below, as it is not the Examiner's job to determine

whether any non-underlined, non-designated amendments are present in the claims.

***Response to Arguments***

2. Applicant's arguments filed 3/10/2009 have been fully considered but they are not persuasive.

Applicant argues that “Scheidt fails to disclose "receiving a request for an access permission security profile on behalf of a network user" as recited in claim 1. Contrary to the Examiner's assertion, no where does Scheidt indicate that a network user makes any requests for the access permission security profile." Nowhere did the Examiner assert that Scheidt teaches a request for an access permission security profile. In fact, the office action explicitly states that Scheidt does not disclose “receiving a request for an access permission security profile”.

Applicant goes on to state that “Scheidt insists that either a smart card .. or a super card .. should be used store and hold this information and be directly connected to a workstation”. First off, Scheidt teaches that a smart card need not be used in all embodiments (the Examiner will refer to "smart card" or “card” as encompassing both the smart card and super card described in Scheidt unless one must be distinguished from the other). For example, column 5, lines 16-18 reads "CKM can be implemented completely in software, using a floppy disk as a token, or it can be implemented with a mix of hardware and software, using a smart card as a token." Clearly, Scheidt does not insist that a smart card need be used (though Applicant does not even argue this, the argument states

that Scheidt insists that a smart card should be used, which may be the case at least in some embodiments, but possible use of a smart card is of no detriment to Scheidt's teachings with respect to the claims).

Applicant further argues that "Scheidt suggests and therefore teaches away from using anything but a smart card or similar storage medium." Applicant goes on to provide arguments regarding the super card of Scheidt. One is left to wonder how explaining benefits of using a super card in some embodiments is meant to teach away from anything in the claims. Furthermore, Scheidt teaches that no smart card or super card need be used with the system. As described above, Scheidt explicitly teaches use of a floppy disk as a token, which clearly does not provide the benefits of local processing that Applicant believes to teach away from "using anything but a smart card or similar storage medium". Further still, Scheidt teaches that "The credentials are stored on the user's card, or in a file or on another type of token, or on a server" (Column 9, lines 61-63). Clearing, storing the credentials in a file or on a server doesn't require use of a smart card or super card. Continuing with Scheidt's teachings, column 14, lines 42-44, reads "The user's credentials are stored either on a token, the user's workstation, or a server." This is deemed to be enough proof that Scheidt clearly and unambiguously teaches that the system can be used without a smart card.

Applicant argues that Scheidt requires that the card be handed directly to the user. However, as just described, the system need not use any card. Furthermore, even in embodiments of Scheidt that do use cards, column 10, lines 19-25, teaches that "Except for the issuance of smart cards and credentials

to new users, reissuance of credentials only requires the transfer of a first use password and new credentials file (if not stored on a server) to the users. The user does not have to be in the presence of the Credentials Manager again. Passwords can be distributed through an existing organizational administrative channel." With reference to Applicant's argument, citing column 9, lines 60-63 as supposedly showing that Scheidt "intentionally requires that the card having the credentials be handed to the user directly as part of a security measure", there is no requirement of such. Indeed, the portion cited by Applicant states that the credentials can be stored in a file or on a server, as previously described. If the credential is stored on a server, it is highly unlikely that the server will be "handed to the user directly" (this is not described in Scheidt, and is certainly not required). Furthermore, Applicant appears to misunderstand the difference between a smart card and a credential. The credential is the data, that can be stored on a smart card, workstation, server, etc. in Scheidt, whereas the smart card is merely a storage medium that may be used in some embodiments of Scheidt for storage of such.

Applicant goes on to argue that "Scheidt assumes the smart card already has the access permission security profile hence there is no reason to then create it on demand", however, the user does not always have the smart card, even in embodiments where Scheidt uses such smart cards. Scheidt describes the secure transmission of the credential's information from the Policy Manger to the Credential Manager, and the distribution of the credential from the Credential Manager to the credential's storage location (e.g. smart card, file, server,

workstation), whether such distribution is to be issuance or reissuance of a credential. Applicant has yet to provide any arguments with respect to embodiments of Scheidt that do not use smart cards, which is a troublesome issue for discussion purposes, however, it is clear from the above that the user is not always in possession of a smart card in Scheidt. In embodiments using smart cards, however, a person must obtain the smart card somehow (possibly by physically handing the card to the user), after a time during which the credential was securely transmitted to the Credential Manager (as described in column 9, lines 53-54, "It is preferable that the user is present at this step", referring to creation of credentials when smart cards are used), and stored on the smart card (by transmission from the Credential Manager or a computing device thereof). Therefore, the credential's information has been securely transmitted to the Credentials Manager, and then further transmitted to the smart card, in embodiments using smart cards. Since a network is an interconnection of devices, both of these transmissions are deemed to be across "networks". The users presence at the Credential Manager clearly correlates to a desire to acquire the credentials and, while not explicitly teaching a request (the rejection does not state that Scheidt teaches such a request, as described above), teaches a time which is after or during which such a request would have been made in the combination, described below (this is not the sole interpretation, however, as timing of the steps is discussed below).

Applicant also argues that Scheidt does not teach or suggest "securely transmitting the access permission security profile to the network user over the

network." As just described, Scheidt does teach such transmission. However, reference to "the network" of the claim is not to be confused with reference to "the network" in rejections citing Scheidt. As described in the rejection, and as just described (with respect to only a portion of Scheidt, there are more teachings, as will be described), Scheidt teaches such secure transmission occurring over a network, however, does not explicitly disclose that the network is a decentralized public network. The combination shows He as teaching such decentralized public network. As for the secure transmission, other than the portions just described, this response previously cited column 10, lines 19-25, which clearly and explicitly shows transmitting a first use password and new credentials file to the users without the users being in the presence of the Credential Manager. Further, with respect to this creating occurring after the request, the timing is deemed insignificant, as the claims do not refer to any such requirement on timing. A user may request a credential today, and not receive the credential created in the creating step of claim 1 for 3 years. Therefore, any reissuance of credentials in Scheidt will clearly fall under the secure transmitting of a profile.

As one can see, Scheidt clearly contemplates transmission of credentials over networks, even in embodiments using smart cards, and recommends to do so in some circumstances.

Applicant goes on to argue that "To combine He with Scheidt would defeat the security aspect of scheidt requiring that the smart card, super card or other storage device must be used to hold a access permission security profile". As

described numerous times already, Scheidt does not require use of a smart card or super card. Applicant has not described "storage device" clearly enough within this argument to provide a response thereto, however, the Examiner is interpreting this argument in a like manner to the previous arguments made by Applicant that erroneously contend that a smart card or another form of portable storage device must be used within Scheidt. Even in embodiments of Scheidt using smart cards, the combination of Scheidt in view of He is proper.

Applicant argues that "He concerns controlling access to "network elements" and does not teach or suggest anything about requesting and receiving access permission security profiles." As noted in the rejection, Scheidt teaches such access permission security profiles, and such teaching has not been argued. Therefore, He does not need to also teach such profiles. One entity of He that can correspond to the access permission security profile of the claims (e.g. credentials in Scheidt) is the list of credentials in He. Clearly, one can see the correspondence between credentials and lists of credentials. Applicant goes on to argue that He "does not actually provide the ability to gain access to information, network elements or anything" after arguing that He discloses controlled access for network elements. These arguments are contradictory, as Applicant argues that He discloses controlling access to network elements, but also argues that He does not disclose the ability to gain access to network elements. He is concerned with providing access to network elements and providing data to users, such that authorized users may acquire such data.

Applicant argues that there is no basis for the motivation to combine He with Scheidt without any reasoning as to why Applicant believes this. Upon reviewing He, one will readily realize that He teaches creation and/or transmission of credentials (corresponding to the security profile) after authenticating and authorizing the user for such credentials, wherein the credentials are stored on a server and accessed by the user from a variety of devices. These are clearly benefits to the system of Scheidt in that additional security is provided when the credentials are stored on a server, for example, as explicitly recited in Scheidt (described above). Therefore, the motivation and combination are proper. Applicant goes on to "request the Examiner to withdraw the rejection if the source of these many limitations cannot be identified." The Examiner is unsure how to respond to this request, as no "limitations" are provided in the motivation. The motivation to combine references is just that, a motivation as to why one of ordinary skill in the art would combine the teachings of multiple references in order to obtain a certain end result. The limitations of the claims were clearly shown as corresponding to portions of He as well. Without knowing what Applicant is requesting, it is difficult to respond to such a request. Assuming Applicant wishes to know where the motivation arises in He, the portions of He cited in rejection of the claimed limitations provide such motivation. As one can easily see from the cited sections, He authenticates and authorizes the user, then provides the list of credentials to the user from the credential server to whatever device the user is currently using. This clearly provides the benefits of central storage (on the credential server) of the

credentials and transmission of such credentials only after authentication and authorization. Furthermore, many other portions of He discuss such benefits. For example, column 1, lines 59-63 describe how the centralized user administration and credential control is highly desirable to large and complex networks, clearly showing the benefit of providing a centralized server storing the credential and from which the user will request such credential. Various other portions show such motivation, however, the above clearly shows that the motivation is found within He.

Applicant provides various arguments related to column 7, lines 41-54. Applicant argues that "One skilled in the art at the time of He would most definitely not consider actually sending an access permission security profile to a user over a network as that would not be ensuring physical security." As described above, and as noted by Applicant, He provides a list of credentials from the credential server to the user. Therefore, He clearly and explicitly sends the credentials (corresponding to the profile of the claims and credentials of Scheidt, for example) across the network.

Applicant further argues, with respect to column 7, lines 41-54, that "based on this aspect of what He does teach, it would follow that access permission security profiles should never be separated from a smart card or transmitted over the Internet. Those skilled in the art at the time of He believed that no security was possible over a network unless physical security were somehow assured." Applicant is making an erroneous interpretation of the portions cited in column 7. For example, Applicant is arguing that the cited paragraph teaches that no

security is possible for data being transmitted across a network. However, He's true teaching is that no security is possible for the network itself. This is the only conclusion one of ordinary skill in the art would make upon reading this paragraph. This is made quite clear in the paragraph, as well as the context thereof in the document. For example, this paragraph states that "The security of the interconnection network that enables users to access network resources and information in the network elements shall never be automatically assumed in any comprehensive solution to the protection of network resources and information. This is simply because it is impossible to physically secure each and every single link of the network." These sentences clearly and unambiguously separate security/protection of the network from security/protection of the network resources and information to be communicated across the network. This is quite clear from the sentence describing that it is impossible to physically secure each and every single link of the network, as well as the previous sentence describing the difference between the network and information/resources. He also states in this citation that "no attempts to secure the interconnection network shall ever be pursued, for they are never be achievable except in very few isolated instances where the interconnection network can be physically constrained in an area where physical security can be assured." This sentence clearly describes that no attempts are made to secure the physical network itself, except in instances where the network can be physically constrained (and thus, physically protected). Furthermore, He is concerned with securing information transmitted across such insecure links. For example, column 9, line 63 to column 10, line 3 reads

"Encryption and decryption provides the necessary means for the protection of network information from being disclosed to those users who are not authorized to receive and retrieve it. It can be used as a supplement to access control mechanisms against unauthorized information disclosure but is primarily used for conducting secure communications between users and network elements in a networking environment." This citation and many other portions of He show that He is concerned with the protection of information across network links. The need for such protection via access control, encryption, and the like, is because of the issue discussed in column 7, lines 41-54, in that the physical networks themselves are never assumed to be secure.

Applicant continues this argument, stating that "one skilled in the art would not attempt to send a access permission security profile over the Internet or other network since it would not be possible to assure physical security along the way." As just described, He is fully concerned with protecting information transmitted across networks, since the networks cannot be physically secured. Applicant's argument is ludicrous, particularly when He does send the credentials or profiles (profiles are described in column 2, lines 24-30, for example as including credentials) across networks that cannot be physically secured. The entire point of He is to provide access control and protection of data across networks that cannot be physically secured by providing means of securing the data itself.

Applicant argues that "He teaches away from transmission of a security profile over a network". As just described, and as provided in the cited portions, He clearly teaches retrieving "the list of user credentials from the registration

database 210 and enclose the list in a credential ticket. The credential ticket is sent back in a response message and will be used for the user to communicate with the network element access server 206" (Column 19, lines 3-8). Further down, this paragraph states that "The message is encrypted with the temporary user-credential server secret key so that only the correct user is able to retrieve the needed ticket and other information from the response message." The credential server sends a response message back to the user, such message including credentials, which correlate to the credentials/profile of Scheidt, such message being encrypted. There is no other way to interpret this, He unambiguously teaches sending of the credential in a secure transmission over a decentralized public network (e.g. one that cannot be physically secured).

Applicant argues that Scheidt does not teach a system having "a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network" since Scheidt describes using cards to store this information in advance rather than distribute over a network. The Examiner is unsure what distribution of a credential over a network or storing the credential on a smart card has to do with "a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network". There is no distribution of any credentials, capabilities, or profile over any network, storage of such on a smart card, of anything that would relate these concepts of transmission and storage within this limitation. Scheidt clearly teaches "a plurality of member tokens for providing cryptographic capabilities to authenticated users over a network", as described in the rejection. Applicant also

states that "The Examiner supports this assertion and admits that Scheidt does not teach or suggest a method or system for distributing cryptographic capabilities over a decentralized public network." The Examiner never made such an admission, as is clear from the rejections. Applicant goes on to argue that "Schwartz also does not teach, suggest or even describe any details related to key management or distributing cryptographic capabilities over a decentralized public network for at least the reasons previously described." However, Shwartz has not been discussed previously, so there are no reasons previously described with respect to Shwartz.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 52-58 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 52 now recites "the system responsive to instructions executable on at least one processor associated with the system". However, no such instructions or processor(s) are found in the application as originally filed, nor

does the application as originally filed describe any system being responsive to such instructions executable on such processor(s).

### *Claim Rejections - 35 USC § 101*

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 52-58 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 52 recites "A centralized security management system .., the system responsive to instructions executable on at least one processor associated with the system". This processor is not part of the system and, therefore cannot be a physical component of the system in order to make the claim statutory. The at least one processor is "associated with the system" and the system if "responsive to" instructions executable on at least one processor. The system of claim 52 has no physical components and, therefore, is non-statutory. Claims 53-58, dependent from claim 52, provide no physical components, and are also non-statutory.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been

obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-20, 52-57, and 59-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt (U.S. Patent 6,490,680) in view of He (U.S. Patent 6,088,451) and Shanton (U.S. Patent 5,680,452).

Regarding Claim 1,

Scheidt discloses a method for providing cryptographic capabilities to a plurality of network users over a network, the method comprising:

An access permission security profile that gives the network user the ability to access one or more objects associated with a domain according to the network user's membership in one or more groups within the domain (Column 7, line 59 to Column 8, line 9; and Column 8, line 63 7to Column 9, line 65);

Authenticating the network user according to an n-factor authentication suitable to the plurality of network users and verifying membership in the domain and the one or more groups (Column 7, lines 29-43; and Column 14, lines 24-38);

Creating the access permission security profile having an ephemeral cryptographic characteristic and derived from a combination of the user's membership in the one or more groups (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67), wherein the combination of the user's membership in the one

or more groups can be used to form a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object when one or more groups associated with the encrypted object match the network user's membership in one or more groups within the domain (Column 10, line 53 to Column 11, line 12; and Column 17, lines 15-65) and to encrypt selected portions of a plaintext object to be accessed by other network user when the other network users' membership in one or more groups within the domain also match the one or more groups associated with the selected portions of the plaintext object being encrypted (Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14); and

Securely transmitting the access permission security profile to the network user over the network wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptographic operations for a predetermined period of time (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12);

But does not explicitly disclose that the network is a decentralized public network or receiving a request for an access permission security profile and authenticating such request, or providing access to different portions of an object to different

entities accessing the same object (though this is not necessarily claimed).

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67);

Receiving a request for an access permission security profile on behalf of a network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and

Authenticating the request from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses providing different access control to portions of objects, such that an different portions of an object may be accessed differently by each entity authorized to access the object (Abstract; Column 8, lines 1-26; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the

embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 2,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities according to each network user's membership in a particular combination of groups within the domain (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Establishing one or more access codes for each group in the domain, wherein each access code is adapted to be combined with other components to form the cryptographic key (Column 4, line 51 to Column 5, line 2; Column 8, lines 31-44; and Column 10, line 53 to Column 11, line 12); and

Creating one or more access permission security profiles for each network user based on membership in one or more different

combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence with the network user's membership in at least one group in the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 3,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, or workgroup within the domain (Column 8, lines 31-44).

Regarding Claim 4,

Scheidt discloses a method for providing decryption capabilities to a plurality of network users over a network, the method comprising:

Decryption capabilities associated with a network user that gives the network user the ability to decrypt one or more encrypted objects associated with a domain according to the network user's membership in one or more groups within the domain (Column 7, line 59 to Column 8, line 9; and Column 8, line 63 to Column 9, line 65);

Authenticating the network user according to an n-factor authentication suitable to the plurality of network users and

verifying membership in the domain and the one or more groups (Column 7, lines 29-43; and Column 14, lines 24-38);

Creating an access permission security profile derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key and decrypt selected portions of the one or more encrypted objects (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67);

Receiving information associated with the selected portions of an encrypted object (Column 10, lines 45-67; Column 16, line 34 to Column 17, line 36);

Generating a cryptographic working key using the cryptographic key associated with the access permission security profile and the received information associated with the selected portions of the encrypted object (Column 10, lines 45-67; Column 16, line 34 to Column 17, line 36); and

Securely transmitting the cryptographic working key to the network user over the network allowing the network user to decrypt the selected portions of the encrypted object (Column 10, lines 45-67; Column 16, line 34 to Column 17, line 36);

But does not explicitly disclose that the network is a decentralized public network or receiving a request for decryption capabilities and authenticating such request, or providing access to

different portions of an object to different entities accessing the same object (though this is not necessarily claimed).

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67);

Receiving a request for an decryption capabilities on behalf of a network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and

Authenticating the request from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses providing different access control to portions of objects, such that an different portions of an object may be accessed differently by each entity authorized to access the object (Abstract; Column 8, lines 1-26; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the

embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 5,

Scheidt as modified by He and Shanton discloses the method of claim 4, in addition, Scheidt discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities according to each network user's membership in a particular combination of groups within the domain (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Establishing one or more access codes for each group in the domain, wherein each access code is adapted to be combined with other components to form the cryptographic key (Column 4, line 51 to Column 5, line 2; Column 8, lines 31-44; and Column 10, line 53 to Column 11, line 12); and

Creating one or more access permission security profiles for each network user based on membership in one or more different

combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence with the network user's membership in at least one group in the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 6,

Scheidt as modified by He and Shanton discloses the method of claim 4, in addition, Scheidt discloses that each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, or workgroup within the domain (Column 8, lines 31-44).

Regarding Claim 7,

Scheidt discloses a method for cryptographically securing the distribution of information over a network to a plurality of network users, the method comprising:

Creating a computer representable data object (Column 4, line 51 to Column 5, line 2);

Associating a pseudorandom cryptographic key with the data object (Column 7, lines 44-58; Column 10, lines 45-67; and Column 16, line 11 to Column 17, line 14);

Encrypting the object using a working key derived from the pseudorandom cryptographic key associated with the object and

other components (Column 7, lines 44-58; Column 10, lines 45-67; and Column 16, line 11 to Column 17, line 14);

Creating a set of one or more access permission credentials that identify the roles each of the plurality of network users may possess in a domain and their membership in one or more groups as defined by various combinations of the one or more access permission credentials (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67);

Assigning a member credential to the object, wherein the member credential is a specific combination of the one or more access permission credentials ensuring that only network users having a matching member credential are able to decrypt the data object (Column 16, line 11 to Column 17, line 50);

Inserting the pseudorandom cryptographic key in a header of the object after first encrypting the pseudorandom cryptographic key with a credential key derived from the member credential associated with the object (Column 16, line 11 to Column 17, line 14);

Transmitting the data object over the network having the encrypted pseudorandom key inserted in a portion of the object (Column 16, line 11 to Column 17, line 14); and

Securely transmitting an access permission security profile, having an ephemeral cryptographic characteristic, to at least one

network user from the plurality of network users wherein the access permission security profile for the at least one network user can be used to generate a credential key capable of decrypting the encrypted pseudorandom cryptographic key associated with the encrypted object because the member credential of the network user matches the member credentials associated with the encrypted object, wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptographic operations for a predetermined period of time (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12);

But does not explicitly disclose that the network is a decentralized public network or the usage of embedded objects within an object.

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such

that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses including one or more embedded objects in a data object (Abstract; Column 8, lines 1-42; and Column 9, line 63 to Column 10, line 10);

Associating a pseudorandom key with each of the one or more embedded objects of the data object (Abstract; Column 8, lines 1-42; and Column 14, lines 7-32);

Encrypting each of the embedded objects using a working key derived from the pseudorandom cryptographic key associated with the embedded object and other components (Abstract; Column 8, lines 1-42; and Column 14, lines 7-32);

Assigning a member credential to each of the selected embedded objects so that only a user with a matching credential can decrypt encrypted embedded objects of the object (Abstract; Column 8, line 1-42 to Column 9, line 23; and Column 14, lines 7-32); and

Inserting a pseudorandom key in a header of each embedded object (Abstract; Column 6, lines 7-39; Column 8, lines 1-42; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to

allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 8,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, Scheidt discloses that the information is digital content (Column 7, lines 12-27).

Regarding Claim 9,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, He discloses that securely transmitting further includes receiving a request for an access permission security profile on behalf of a network user and authenticating the request from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and Scheidt discloses authenticating users using an n-factor authentication suitable to authenticate the plurality of network users (Column 7, lines 29-43; and Column 14, lines 24-38).

Regarding Claim 10,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, He discloses that securely transmitting further includes sending a request for an access permission security profile on behalf of a network user to a

centralized server system over the network; receiving the request on behalf of the network user at the central server system; and authenticating the request as from the network user (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64); and Scheidt discloses authenticating users using an n-factor authentication suitable to authenticate the plurality of network users (Column 7, lines 29-43; and Column 14, lines 24-38).

Regarding Claim 11,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, Scheidt discloses that the step of securely transmitting an access permission security profile is not performed if the user already has possession of an access permission security profile (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12).

Regarding Claim 12,

Scheidt as modified by He and Shanton discloses the method of claim 7, in addition, Scheidt discloses that the working key may further be derived from at least a domain component, a maintenance component, and the pseudorandom key (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

Regarding Claim 13,

Scheidt as modified by He and Shanton discloses the method of claim 10, in addition, Scheidt discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 4, line 51 to Column 5, line 2; Column 8, lines 31-44; and Column 10, line 53 to Column 11, line 12); and

Creating one or more access permission security profiles for each network user based on membership in one or more different combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence with the network user's membership in at least one group in the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 14,

Scheidt as modified by He and Shanton discloses the method of claim 13, in addition, Scheidt discloses that each group is a category, organization, organizational unit, set of role based

credentials, work project, geographical location, or workgroup within the domain (Column 8, lines 31-44).

Regarding Claim 15,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, or 9, in addition, He discloses that the request is initiated in-band by the network user over the network (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64).

Regarding Claim 16,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, 10, or 11, in addition, Scheidt discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 17,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of biometric identification (Column 12, line 46 to Column 13, line 19).

Regarding Claim 18,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of a hardware token (Column 11, lines 22-30; and Column 11, line 65 to Column 12, line 46).

Regarding Claim 19,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of a software token (Column 14, lines 30-45).

Regarding Claim 20,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 9, or 10, in addition, Scheidt discloses that the authenticating step includes the use of a user password (Column 11, lines 14-20).

Regarding Claim 52,

Scheidt discloses a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a network, they system responsive to instructions executable on at least processor associated with the system and further comprising:

A plurality of member tokens for providing cryptographic capabilities to authenticated users of the network (Column 7, line 59 to Column 8, line 9; and Column 8, line 63 to Column 9, line 65);

A set of server systems for managing the distribution of the member tokens (Column 7, line 13 to Column 9, line 24);

A set of client systems, wherein each client system includes means for receiving a member token and means for utilizing the

cryptographic capabilities provided by the member token for selective encryption and decryption (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12); and

Means for securely distributing a member token from at least one server system to at least one client system over the network (Figure 6; Column 4, lines 7-14; Column 8, line 46 to Column 10, line 25; and Column 10, line 53 to Column 11, line 12);

But does not explicitly disclose that the network is a decentralized public network, means for requesting a member token from at least one server system, or providing access to different portions of an object to different entities accessing the same object (though this is not necessarily claimed).

He, however, discloses that the network is a decentralized public network (Figure 10; and Column 30, lines 47-67); and

Means for requesting a member token from at least one server system (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security system of He into the access control system of Scheidt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized

before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.

Shanton, however, discloses providing different access control to portions of objects, such that an different portions of an object may be accessed differently by each entity authorized to access the object (Abstract; Column 8, lines 1-26; and Column 14, lines 7-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the access control system of Scheidt as modified by He in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded object.

Regarding Claim 53,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, Scheidt discloses that each client system further includes user authentication means (Column 11, lines 14-40).

Regarding Claim 54,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, He discloses that the means for

requesting a member token resides on each client system (Column 18, line 33 to Column 19, line 15; and Column 25, lines 21-64).

Regarding Claim 55,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, Scheidt discloses that means for authenticating a user resides on at least one server system (Column 7, lines 13-58; and Column 13, lines 22-36).

Regarding Claim 56,

Scheidt as modified by He and Shanton discloses the system of claim 52, in addition, Scheidt discloses that managing the distribution of the member tokens includes dynamic updating of the member tokens (Column 8, line 46 to Column 10, line 25).

Regarding Claim 57,

Scheidt as modified by He and Shanton discloses the method of claim 1, 4, 7, or the system of claim 52, in addition, He discloses that the decentralized public network is the Internet (Figure 10; and Column 30, lines 47-67).

Regarding Claim 59,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the access permission security profile received by the network user remains encrypted on a persistent memory device until decryption of one or more portions of the access permission security profile is deemed

necessary to effectuate performing one or more cryptographic operations on one or more objects (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 65).

Regarding Claim 60,

Scheidt as modified by He and Shanton discloses the method of claim 59, in addition, Scheidt discloses that the access permission security profile may be decrypted when the network user in receipt of the access permission security profile successfully performs an n-factor authentication operation (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 65).

Regarding Claim 61,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the network user in receipt of the access permission security profile can no longer perform cryptographic operations on one or more objects when the predetermined period of time associated with the ephemeral cryptographic characteristic has expired (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 62,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that the network

user in receipt of the access permission security profile can not perform cryptographic operations on one or more objects when one or more groups associated with the encrypted object do not match the network user's membership in one or more groups within the domain (Column 8, line 46 to Column 10, line 25; and Column 10, lines 53-67).

Regarding Claim 63,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that decrypting selected portions of the encrypted object with the access permission security profile produces a secondary cryptographic key to be used in further decrypting the selected portions of the encrypted object (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 65).

Regarding Claim 64,

Scheidt as modified by He and Shanton discloses the method of claim 1, in addition, Scheidt discloses that encrypting selected portions of the plaintext object includes encrypting a randomly generated value with respect to the one or more groups associated with plaintext object to be encrypted (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

Regarding Claim 65,

Scheidt as modified by He and Shanton discloses the method of claim 2, in addition, Scheidt discloses that the network user's membership in one or more different combination of groups corresponds to member credentials associated with the network user and selected from a set of access permission credentials associated with the domain (Column 4, line 51 to Column 5, line 2; Column 10, line 53 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

Regarding Claim 66,

Scheidt as modified by He and Shanton discloses the method of claim 65, in addition, Scheidt discloses that encrypting selected portions of the plaintext object includes encrypting the plaintext object using a randomly generated value (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14);

Generating a pseudorandom value by encrypting the randomly generated value in combination with one or more different credentials selected from the set of access permission credentials associated with the domain (Column 7, lines 44-58; Column 10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14); and

Embedding the pseudorandom value in the selected portions of the encrypted plaintext object (Column 7, lines 44-58; Column

10, line 45 to Column 11, line 12; and Column 16, line 11 to Column 17, line 14).

6. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt in view of He and Shanton, further in view of Win (U.S. Patent 6,161,139).

Regarding Claim 21,

Scheidt as modified by He and Shanton may not explicitly disclose that the authenticating step includes the use of a record of time at which the request was made.

Win, however, discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the RBAC system of Win into the access control system of Scheidt as modified by He and Shanton in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

Regarding Claim 22,

Scheidt as modified by He and Shanton may not explicitly disclose that the authenticating step includes the use of a record of the user's physical location.

Win, however, discloses that the authenticating step includes the use of a record of the user's physical location (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the RBAC system of Win into the access control system of Scheidt as modified by He and Shanton in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

7. Claim 58 is rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt in view of He and Shanton, further in view of Anderson (U.S. Patent 5,805,674).

Scheidt as modified by He and Shanton does not explicitly disclose that the decentralized public network is a cellular phone network.

Anderson, however, discloses that the decentralized public network is a cellular phone network (Column 11, line 62 to Column 12, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the cell phone security system of Anderson into the access control system of Scheidt as modified by He and Shanton in order to allow the system to increase a level of authentication in response to suspicious events (such as, by requiring biometrics where a password would normally suffice).

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437